Appendix B
References

Appendix Overview

Numerous sources of information were consulted in preparing this revision of the Systems Development Life Cycle Handbook.

In This Appendix

The following types of information are summarized in this appendix.

Section A
Government Reference Documents Synopses

Overview

This section summarizes the directives, standards, and other publications applicable to Customs applications development.

Additional Standards

If your application is highly specialized, additional standards may be applicable. A good source for determining if standards exist for all or part of the application you are developing is the FIPS Index, published by the National Technical Information Service (NTIS). A copy of this directory and the Code of Federal Regulations are located in the reference section of the Customs library at Headquarters.

In This Section

Source	See Page
Customs Directives	IV-B-3
Customs Enterprise Architecture Documents	IV-B-5
Treasury Directives	IV-B-6
General Services Administration (GSA) Publications	IV-B-7
Code of Federal Regulations (CFR), Federal Information Resources Management Regulations (FIRMR)	IV-B-7
OMB Circulars	IV-B-8
Federal Information Processing Standards (FIPS)	IV-B-10
National Computer Security Center Guidelines	IV-B-14

Customs Directives

Availability

Customs Directives are available on-line from the mainframe through the Customs Issuance System (CIS). All directives in the CIS are prefixed with “099". A directory of applicable directives will be displayed if you enter “IM” in the data field labeled “Issuing Office”.

Directive HB 1400-05

Automated Information System Security Policy Manual: This manual provides general security procedures and policies to be used with Customs automated information systems.

Directive 5510-10

Applications System Life Cycle Management: This directive adopts Treasury Directive 84-01 and Treasury Manual TD P 84-01 as the standard for Customs.

Directive 5510-15

GOSIP Government Open Systems Interconnection Profile: This directive adopts FIPS Publication 146-1, Government Open Systems Interconnection Profile (GOSIP), as the customs standard for inter-connection compatibility. (FIPS 146-1 has been withdrawn in preference to the proposed Application Portability Profile.)

Directive 5510-23

U.S. Customs Information Resource Management (IRM) Review Program: This directive establishes the requirement and methodology for conducting reviews of Customs information resources to ensure that the resources are being utilized efficiently and effectively. This directive requires quarterly status reports for the current fiscal year reviews, and also annual review reports must be provided to Treasury for subsequent reporting to GSA, GAO, OMB, etc.

Directive 5510-24

Local Management Information Systems (MIS) : This directive establishes policy to upgrade the national inventory of local MIS, and establishes criteria covering the development of a local MIS is not appropriate.

Directive 5510-25

Policies and Procedures for Customs Information Technologies (IT) Acquisitions: This directive establishes a uniform set of policies and procedures for Information Technology (IT) acquisitions throughout the U.S. Customs Service.

Continued on next page

Customs Directives, Continued

Directive 5510-26

Customs Electronic Data Retention and Schedules: This directive establishes a service wide policy for the storage of Customs electronic data. This policy provides storage life-cycle schedules for keeping historical data on-line, archiving the data for long-term storage, destroying the data or transferring it to the National Archives Records Administration Federal Records Center for permanent retention.

Customs Enterprise Architecture Documents

Overview

These documents were created to assist the United States Customs Service in its migration towards an integrated enterprise IT Architecture by the Cambridge Technology Partners.

Executive Overview

U.S. Customs Service Enterprise IT Architecture Strategy Executive Overview [v1.0], August 29, 1997.

Application Migration Strategy

U.S. Customs Service Application Migration Strategy [v1.0], July 21, 1997.

Infrastructure Migration Strategy

U.S. Customs Service: Customs Infrastructure Migration Strategy [v1.0], July 21, 1997

Process

U.S. Customs Service: Process for Cost Benefit Analysis, Master Schedule, and Investment Alternatives [v1.0], July 21, 1997

Organization Migration Strategy

U.S. Customs Service Organization Migration Strategy [v1.0], July 21, 1997

Technology Policy

U.S. Customs Service: Customs Technology Policy, [v1.0], July 21, 1997.

Technology Portfolio

U.S. Customs Service Technology Portfolio [v1.0], July 21, 1997.

Treasury Directives

Directive
TD 25-04

Implementation of the Privacy Act of 1974, as Amended: This directive restates policy and procedures and assigns responsibilities for carrying out the requirements of the Privacy Act and authorizes TD P 25-04, “Privacy Act Handbook.

Publication
TD P 25-04

Privacy Act Handbook: Contains detailed definitions of and procedures for Privacy Act Systems of records. Includes the text of the Privacy Act, Treasury Disclosure regulations and TD 25-04 as Appendices.

Publication
TD P 71-10

Department of the Treasury Security Manual: The primary purpose of this manual is to establish comprehensive, uniform security policies, procedures, and guidelines to be followed by each bureau in developing its own specific policies and operating directives.

Publication
TD P 83-01

Guidelines for Acquiring Federal Information Processing Resources: This directive provides guidelines for procurement decisions of ADP hardware and proprietary software. It establishes a requirement for certain documents, including the Mission Needs Statement (MNS), Cost/Benefit Analysis and Requirements Analysis, to be used in making a procurement decision.

Publication
TD P 84-01

Information System Life Cycle Manual: Describes the procedures applicable to managing the full system development life cycle for Treasury ADP systems and/or applications. It addresses the aspects of requesting, identifying, defining, testing and implementing ADP systems and applications in varying levels of detail.

Publication
TD P 85-03

Risk Assessment Guideline, Vol 1 & 2: This directive provides guidelines for identifying and quantifying potential areas of risk for ADP hardware and application software. It also provides a methodology for determining how to establish baselines for risk exposure and to minimize damage due to compromise, natural disaster, and system failure.

Directive
TD 87-01

Information Systems Standards Program: This directive restates policy and delineates responsibilities for the Treasury Information Systems Standards Program.

General Services Administration (GSA)

Publication

A Model IRM Program: Provides a model IRM methodology based on a long term study of the 30 largest government IRM services, that are provided to users. Included were all military services, Treasury, Agriculture, OPM, etc. Publication shows Application Life Cycle Steps as they were actually done rather than through theoretical approach. A special section identifies approaches that were less than fully successful on previous projects. This can help developers avoid these problems in the future.

Code of Federal Regulations (CFR), Federal Information Resources Management Regulations (FIRMR)

CFR 41, (Chapter 201-1.000-1 — 201-33.012

Federal Information Resources Management Regulations: Identifies aspects of ADP functions and operation, including hardware acquisition and disposal, software development (internal vs. external), and security measures (physical and software), etc. This subject descriptions are general in nature, leaving compliance procedures to the individual agencies. Current Treasury directives and Customs handbook already comply with applicable CFR guidelines.

FIRMR Bulletin 90-3

Replacement of, and Screening For, Federal Information Processing (FIPS) Equipment Under Exchange/Sale Authority: This bulletin outlines procedures to be used in conjunction with exchange/resale of Federal Information Processing equipment no longer required by a Federal office or agency.

OMB Circulars

Circular A-11 **Preparation and Submission of Budget Estimates**: Prescribes policies and procedures for preparing and submitting agency budgets to the Executive Branch.

Circular A-34 **Budget Execution**: Prescribes policies and procedures for executing budgets once approved and authorized by Congress and the Executive Branch.

Circular A-76 **Performance of Commercial Activities - Sections I and III**: These sections describe criteria to consider when performing a management study to determine whether an ADP system is needed.

Circular A-94 **Discount Rates to be Used in Evaluating Time-Distributed Costs and Benefits**: This circular establishes policy and sets guidelines for calculating depreciation and amortization of Federal tangible assets when evaluating costs and benefits. This circular is re-issued annually.

Circular A-120 **Guidelines for the Use of Advisory and Assistance Services**: This circular establishes policy and sets guidelines for the appropriate use of advisory and assistance services obtained by contracts. It specifically identifies the types of services allowed to be contracted as well as delineating those actions prohibited from being contracted.

Circular A-123 **Management Accountability and Control**: This circular provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on management controls.

Circular A-127 **Financial Management Systems**: This circular identifies policies and procedures that must be followed when developing, operating, evaluating, or reporting on financial management ADP applications. It also provides specific objectives that financial management systems must meet to comply with applicable law and guidelines from GAO, Treasury and OMB.

Continued on next page

OMB Circulars, Continued

Circular A-130, Appendix III

Security of Federal Automated Information Systems: This appendix requires that appropriate security procedures be put in place for any automated information system and that the procedures will comply with all applicable security standards. It further requires that the procedures by adequately documented and . It divides security functions into four categories: applications, personnel, information technology, and installation. It also calls for security awareness and training.

The primary action required is management certification that the procedures implemented comply with all regulations and standards. This creates a chain of accountability for all security measures in place. As part of this accountability, periodic reviews and re-certification of the security measures in use must be performed, although no intervals are specified.

Federal Information Processing Standards (FIPS)

FIPS Publication 11-3

Guidelines: American National Dictionary for Information Processing Systems: This standard adopts ANSI Standard X3TR-1-82, which establishes standard definitions of terms applicable to information processing systems.

FIPS Publication 31

Guidelines for Automatic Data Processing Physical Security and Risk Management: This publication provides direction for developing physical security and risk management methodologies for ADP facilities.

FIPS Publication 38

Guidelines for Documentation of Computer Programs and Automated Data Systems: This standard identifies and describes ten documents that should be completed to support applications development. These are: Functional Requirements, Data Requirements, System/Subsystem Specification, Program Specification, Data Base Specification (when applicable), Users Manual, Operations Manual, Program Maintenance Manual, Test Plan, and Test Analysis Report. Depending on the nature and size of a given application, some of these may not be required as stand-along documents.

NOTE: The standard permits combining several documents into a single document where circumstances do not warrant separate publications. However, the subject matter of these documents provides a thorough foundation for establishing and maintaining any system and should be addressed in some way.

FIPS Publication 39

Glossary for Computer Systems Security: This publication contains definitions for terms pertaining to ADP privacy and computer security matters.

FIPS Publication 41

Computer Security Guidelines for Implementing the Privacy Act of 1974: This publication provides guidelines for selecting methods to protect data in ADP systems. Specific categories of risk and the safeguards to be implemented for each type, including physical security (access), information management (passwords, etc.) And system controls.

FIPS Publication 49

Guidelines on Computer Performance Management - An Introduction: This publication specifies responsibilities for ADP managers in meeting user requirements, managing and planning resource requirements, informing upper management, and interacting with vendors.

Continued on next page

Federal Information Processing Standards (FIPS), Continued

FIPS Publication 56

Guidelines for Managing Multi vendor Plug Compatible ADP Systems: This provides guidelines for ADP managers responsible for developing ADP systems or applications involving multiple vendors to ensure compatibility and prevent adverse impact to other systems.

FIPS Publication 64

Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase: Provides subject matter for three documents to be produced in the initiation phase of ADP resource selection and development plans: project request, feasibility study, and cost/benefit analysis.

FIPS Publication 65

Guidelines for Automated Data Processing Risk Analysis: Describes how to conduct a risk analysis of ADP equipment and applications, including factors to consider and assessment of loss for different categories of failure.

FIPS Publication 73

Guidelines for Security of Computer Applications: Describes the categories of security that must be considered when developing an ADP system or application. Identifies decisions that should be made at each point in development, and describes some control measures that can be used. Related to FIPS 41 and FIPS 65.

FIPS Publication 77

Guidelines for Planning and Management of Database Applications: This guideline provides methodologies for planning and managing a database application.

FIPS Publication 87

Guidelines for ADP Contingency Planning: this document is fairly old (March 1981), it remains the primary document on this topic from NIST.

FIPS Publication 88

Guidelines on Integrity Assurance and Control in Database Administration: Identifies methodologies for insuring database integrity and security control as well as procedures for verifying the accuracy and completeness of a database. Discusses matters of user access control, system monitoring, and failure/disaster recovery.

Continued on next page

Federal Information Processing Standards (FIPS), Continued

FIPS Publication 99

Guideline: A Framework for the Evaluation and Comparison of Software Development Tools: This guideline establishes a standardized "checklist" for software features so that prospective users can compare similar software and determine which package best suits their requirements.

FIPS Publication 101

Guidelines for Life Cycle Validation, Verification, and Testing of Computer Software: This guideline describes a plan for integrating validation, verification and testing into the overall development process. It includes a helpful glossary of terms and a very useful outline for developing an effective validation, verification and testing plan.

FIPS Publication 102

Guidelines for Computer Security Certification and Accreditation: Sets forth the methods for establishing security certification and accreditation. Technically, a system or applications dealing with confidential data must be tested and approved by an appropriate security validation procedure before it can be activated.

FIPS Publication 105

Guideline for Software Documentation Management: Explains how to manage the development, production, and maintenance of computer software documentation. Includes checklists and references to other standards applicable to software documentation (FIPS 38 and 64, etc.).

FIPS Publication 106

Guidelines for Software Maintenance: Provides tips on improving the maintainability of application software, such a modularization of programs and including comments within the code describing each segment's function or execution. Include decision criteria for whether to continue maintenance or develop a new application. Also describes maintenance tools that can be used.

FIPS Publication 113

Computer Data Authentication: Specifies a cryptographic authentication algorithm for use in ADP systems and networks where cryptographic authentication is necessary. The algorithm uses the data encryption standard (DES) as defined in FIPS 46-1.

Continued on next page

Federal Information Processing Standards (FIPS), Continued

FIPS Publication 123

Specification for a Data Descriptive File for Information Interchange: Specifies standard file and record formats to be used for data that will be exchanged between dissimilar systems.

FIPS Publication 124

Guidelines on Functional Specifications for Database Management Systems: Intended to assist developers of RFPs to establish correct functional specifications for bidders.

FIPS Publication 132

Guidelines for Software Verification and Validation Plans: Sets forth minimum requirements for verification and validation plans. Helps managers establish minimums for task, inputs, and expected outputs for all aspects of software functions. Helps managers identify critical function performance as well as optional function performance criteria.

FIPS Publication 140

General Security Requirements for Equipment Using the Data Encryption Standard: Adopts Federal Standard (Fed-Std) 1027 as FIPS.

FIPS Publication 161-1

Electronic Data Interchange (EDI): Adopts as a FIP the recognized national and international standards for Electronic Data Interchange (EDI) (X.12 and EDIFACT). In EDI data normally transmitted via paper documents is transmitted electronically according to established rules and formats. The data associated with each type of document (such as purchase orders or invoices) are transmitted with the document as an electronic message. Electronic transmission can be by means of telecommunication or by use of some electronic storage medium (such as magnetic disk or tape). The standard requires that any deviation from the standard document content or format must be submitted to NIST for approval along with a timetable for adopting the standard format. Also asks that documents not currently standardized by the study groups be submitted for evaluation and standardization.

National Computer Security Center Guidelines

NCSC-TG-015 **A Guide to Understanding Trusted Facility Management**: This technical guide provides compute security manufacturers, system evaluators, accreditors, auditors, developers, and end-suers with concepts, relevant procedures, methods, and processes for trusted facilities management.

NCSC-TG-016 **A Guide to Writing Trusted Facility Management**: This technical guide provides computer security manufacturers, system evaluators, accreditors, auditors, developers, and end-users guidance for writing, evaluating, and using a trusted facility manual.

NCSC-TG-026 **A Guide to Writing the Security Features User's Guide (SFUG) for Trusted Systems**: This guide expands on the Trusted Computer System Evaluation Criteria by providing guidance on the development and evaluation of SFUG.

Section B
Other References

Overview

The publications cited in this section served as the basis for our survey of industry “Best Practices”. Individual works are grouped by topic.

In This Section

Life Cycles

DeGrace, Peter and Leslie Hulet Stahl

Wicked Problems, Righteous Solutions: A Catalogue of Modern Software Engineering Paradigms. ISBN 0-13-590126-X. This work presents an overview of a number of software engineering life cycles.

TRW

Process Model for High Performance Trusted Systems in ADA: Phase 1 Technical Report. ARPA Order No. 6414. This report represents the results of a R&D effort funded by DARPA/ISTO to produce a next-generation development paradigm for high-performance, trusted system in ADA. In reality, programming language is irrelevant. This is, however, a good discussion of an incremental life cycle.

Incremental Development of Large ADA Systems: An ADA Process Model: This paper was prepared by Walker Royce for presentation at a TRW conference held in 1989. Again, programming language is irrelevant to the description of the life cycle.

An Advanced Process Model's Application to Trusted X Window System Development. A presentation at the Sixth Annual Computer Security Applications Conference (December 1990) by Bonnie Danner and Ann Marmor-Squires.

An Advanced Process Model's Application to Trusted X Window System Development. A TRW Technical report by Bonnie Danner and Ann Marmor-Squires.

STARS '91: Integrating Reuse Into a Life-Cycle Process. A DARPA-funded briefing by Bonnie Danner. December 1991.

Wetherbe, James C. and Nicholas P. Vitalari

Systems Analysis and Design: Best Practices (Fourth Edition). ISBN 0-314-02679-7. A general purpose text that discusses "Best Practices" as applied to each of the individual stage/phase of software development.

Software Engineering Institute Publications

Paulk, Weber, et. al

The Capability Maturity Model: Guidelines for Improving the Software Process (Version 1.1). ISBN 0-201-54664-7. The Software Engineering Institute is currently developing the next version (2.0), which is expected to be available in late-1997 or early 1998.

Humphrey, Watts S.

Managing the Software Process. ISBN 0-201-18095-2. A useful text on project management techniques, issues, and how to improve our abilities and processes. Includes sections on Project Planning, Estimating, Quality Assurance, Configuration Management, Inspections, Testing, and Defect Prevention.

Object-Oriented Technology

Baudoin, Claude and Glenn Hollowell

Realizing the Object-Oriented Life Cycle. ISBN 0-13-124454-X Presents a case and road map for the adoption of object-oriented technology, tools, and methods. It is a fairly good overview of issues involved in object-oriented technology.

Taylor, David A.

Object-Oriented Information Systems Planning and Implementation. ISBN 0-471-54364-0 Focuses on the interaction between object-oriented technology and the more traditional paradigms, making the case that object-oriented technology can be used in a variety of ways to enhance productivity and user satisfaction.

Booch, Grady

Object Oriented Analysis and Design With Applications (Second Edition). ISBN 0-8053-5340-2 A basic text covering all phases of object-oriented analysis and design. Presents a good description of the key elements of object-oriented technology.

Object Solutions: Managing the Object-Oriented Project. ISBN 0-8053-0594-7. A management level introduction to object-oriented technology with a good descriptions of some of the trade-off decisions that must be made in any object-oriented project.

Prototyping

Reilly, John P. Rapid Prototyping: Moving to Business-Centric Development. ISBN 1-85032-193-0. Focuses on prototyping as a method of requirements definition.

Joint Application Development

Andrews, Dorine C. and Naomi S. Leventhal *FUSION - Integrating IE, CASE, and JAD: A Handbook for Reengineering the Systems Organization.* ISBN 0-13-325333-3. A good reference on the tools and techniques to use JAD in all phases of the life cycle. Written both as an introduction to JAD and as a reference text for a facilitator.

Risk Management

Boehm, Barry W.

IEEE Tutorial: Software Risk Management. ISBN 0-8186-8906-4. Contains both tutorial text and reprinted articles describing industry best practices and examples of risk management applications in the areas of risk definition, management practices, resolution techniques, and implementation throughout the software life cycle. Includes discussions of the use of risk management in the spiral development life cycle model and in prototyping/RAD development.

Naval Undersea Warfare Center Division, Dept. of Navy

Practical Software Measurement: A Guide to Objective Program Insight, version 2.1, March 27, 1996. From the Joint Logistics Commanders, Joint Group on System Engineering. Presents complete guidance on selecting and defining metrics to be used for managing software projects, based on the project's needs and issues.

Software Engineering Institute (SEI)

Draft of the SEI *Guidebook on the Software Acquisition Risk Management Key Process Area (KPA)* (version 0.02). CMU/SEI-97-HB-002. Provides information and suggestions regarding the activities needed to implement a Risk Management program.

Software Engineering Institute (SEI)

SEI Taxonomy-Based Risk Identification. June 1993 paper from SEI which identifies specific risk areas of potential concern for a project. Contains a detailed questionnaire used to interview project members to identify risks.